REMARKS

Claims 22 and 35 have been amended solely to cure typographic errors. Claims 1-3, 5-13, 15, 16, 19-33 and 35-42 are pending. In view of the following remarks, Applicant respectfully requests withdrawal of the rejections and forwarding of the application onto issuance.

The Rejections

Claims 1, 5, 11-12, 37-42 stand rejected under 35 U.S.C § 103(a) as being unpatentable over U.S. Patent No. 6,678,733 to Brown et al. (hereinafter "Brown") in view of U.S. Patent No. 6,609,954 to Moreau.

Claim 2 stands rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of U.S. Patent No. 6,070,243 to See et al. (hereinafter "See") and U.S. Patent No. 6,237,095 to Curry et al. (hereinafter "Curry").

Claim 3 stands rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of See.

Claims 6, 9 and 10 stand rejected under 35 U.S.C §103 (a) as being unpatentable over Brown in view of U.S. Patent No. 6,609,954 to Moreau.

Claim 7 stands rejected under 35 U.S.C § 102 as being anticipated by Brown.

Claim 8 stands rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of Moreau and See.

Claims 13, 15 and 16 stand rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of U.S. Patent No. 6,584,564 to Olkin et al. (hereinafter "Olkin").

Claims 19, 24 and 26 stand rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of U.S. Patent No. 6,115,376 to Sherer et al.

(hereinafter "Sherer).

Claims 20-22 stand rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of Sherer and Olkin.

Claim 23 stands rejected under 35 U.S.C § 103(a) as being obvious over Brown in view of Sherer, Olkin, and U.S. Patent No. 6,304,969 to Wasserman et al. (hereinafter "Wasserman").

Claim 25 stands rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of Sherer and U.S. Patent No. 5,937,068 to Audebert.

Claims 27, 28, 30, 31, 33, 35 and 36 stand rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of Audebert and U.S. Patent No 6,295,361 to Kandansky et al. (hereinafter "Kandansky").

Claim 29 stands rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of Audebert, Kandansky and Wasserman.

Claim 32 stands rejected under 35 U.S.C § 103(a) as being unpatentable over Brown in view of Audebert, Olkin and Biran.

Claim 34 stands rejected under 35 U.S.C §103(a) as being obvious over Brown in view of Audebert, Kandansky and See

Before discussing the Office's rejections in detail, Applicant provides the following discussion of Applicant's disclosure to assist the Office in appreciating the claimed subject matter.

Applicant's Disclosure

Referring to Applicant's Fig. 3, a key generator 345 is associated with the authentication server. It has an administrative interface 350 that allows selection of new keys by a user, and provides keys ***in the form of an executable piece of code***

referred to as key.exe via a network 360 (shown in two places for convenience) such as the Internet, to one or more affiliate servers such as a partner site 370. Partner site may have several servers operating as indicated in Figure 3, all servicing the same network domain. The key generator also provides the keys.xml information to the nexus, where it is stored in the configuration file.

When a new partner site is registered by use of the register server 330, a key is generated for the site and provided by S-MIME secure encrypted email, using standard certification, or physically mailed to operators of the site for installation. ***The key is delivered as an EXE with key data embedded within it.***

An object, such as a COM object handles installation and encryption of the keys. The first key has a version number, such as "1", and is stored by the site in encrypted form in a registry using a piece of information that is specific to the physical machine, such as the MAC address of the first network card. ***The key.exe is used for decrypting tickets while the authentication server is still running.***

Key generator 345 also generates a ***key.exe file*** that can be installed on the partner site servers. The new ***key.exe file*** is sent securely to the partner and received. The ***key.exe file is then run against all servers on the partner site with an "/addkey" parameter*** that installs the new key onto the server while still running. It is added as an additional key with no expiration date.

Next, the partner site ***runs the key.exe file against all servers with a "/makecurrent" parameter*** to make the new key the current key by switching a registry key referred to as keycurrent to the new key version.

Key.exe may also be run against all servers using an "/expire" parameter

prior to receiving a new key to cause a service interruption until new keys are installed. This ensures that no new tickets using an old compromised key are accepted, and the old key can be immediately deleted from all servers.

Claims 1-3

Claim 1 recites a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising [emphasis added]:

- generating a first key having a first version number;
- providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;
- generating a second key having a second version number; and when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number;
- wherein ***said keys comprise key data and executable code for decrypting tickets.***

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

While Applicant agrees that Moreau obscurely embeds a cryptographic key in the executable portion of a software application, Applicant respectfully disagrees with the Office's stated rejection for at least two reasons.

First, Applicant disagrees that Moreau's key ***itself*** comprises key data and executable code. Rather, Moreau states that the key is "obscure[ly] ***embedded***" within the executable portion of a software application. Applicant submits that this is quite different from a key which ***comprises*** key data and ***executable code.*** As outlined above, Applicant's key is, in some embodiments, an executable file, which can be run with or without various switches to accomplish various tasks. For example, running "key.exe /addkey" installs the new key onto the server. Running "key.exe /makecurrent" makes the new key the current key. And running "key.exe /expire" expires the current key. There is ***no indication whatsoever*** that Moreau's embedded key comprises executable code, as does Applicant's. Rather, Moreau ***hides*** his key in the executable portion of a software application to prevent a hacker from obtaining the key, using it to reverse engineer a piece of software, and creating a bogus terminal by use of the reverse-engineered software.

Second, and most important, ***nowhere*** in the rejection of this claim does the Office argue that Moreau teaches a key comprising key data and executable code ***for decrypting tickets***. While the Office argues that Moreau teaches "the use of a key in the form of an executable," the Office does not argue that Moreau's key comprises executable code for decyrpting tickets. Applicant respectfully submits that this omission is understandable, given the fact that Moreau does not even ***hint*** at a key comprising executable code for decrypting tickets (or decrypting anything else, for that matter). Because the Office failed to argue that ***all*** of Applicant's claim features are met, and, because such claim features are not met by the cited references, the Office has failed to make a *prima facie* case of obviousness.

Accordingly, for at least these reasons, this claim is allowable.

Claims 2 and 3 depend from claim 1 and are allowable as depending from

an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are neither disclosed nor suggested by the references as cited and applied by the Office. In addition, given the Office's failure to establish a *prima facie* case of obviousness with respect to claim 1, the further rejections of claim 2 over the combination with See and Curry and of claim 3 over See are not seen to add anything of significance.

Claim 5

Claim 5 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising [emphasis added]:

- generating a first key having a first version number;
- providing tickets encoded consistent with the first key, the ticket having a version number corresponding to the first version number;
- generating a second key having a second version number; and
- when the second key becomes current at a site, providing tickets encoded consistent with the second key, the ticket having a version number corresponding to the second version number;
- wherein ***said keys comprise key data and executable code for decrypting tickets.***

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to

include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claims 6-9

Claim 6 recites a method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising [emphasis added]:

- generating a first key ***in the form of an executable*** having a first version number;
- generating a second key ***in the form of an executable*** having a second version number; and
- providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

In making out the rejection of this claim, the Office states that Brown does not teach that "the key is in the form of an executable." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

The combination of these references does not teach or suggest all of the claim features. Specifically, these references do not teach or suggest first and second keys in the form of an executable. Accordingly, the Office has failed to

establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claims 7 and 8 depend from claim 6 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 6, are neither disclosed nor suggested by the references as cited and applied by the Office. In addition, given the allowability of claim 6, the rejection of claim 8 over the combination with See is not seen to add anything of significance.

Claim 9

Claim 9 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of generating keys that decrypt login tickets that log a user into multiple sites, the method comprising [emphasis added]:

- generating a first key ***in the form of an executable*** having a first version number;
- generating a second key ***in the form of an executable*** having a second version number; and
- providing an indication to a login server identifying which key is current for each site such that the tickets are properly encoded.

In making out the rejection of this claim, the Office states that Brown does not teach that "the key is in the form of an executable." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form

of an executable with the motivation to improve the security of the system."

The combination of these references does not teach or suggest all of the claim features. Specifically, these references do not teach or suggest first and second keys in the form of an executable. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claim 10

Claim 10 recites a system that generates keys that decrypt login tickets that log a user into multiple sites, the system comprising [emphasis added]:

- a key generator that generates a first key ***in the form of an executable*** having a first version number and generates a second key in the form of an executable having a second version number; and
- means for providing information to a login server identifying which key is current for each site such that the tickets are properly encoded.

In making out the rejection of this claim, the Office states that Brown does not teach that "the key is in the form of an executable." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

The combination of these references does not teach or suggest all of the claim features. Specifically, these references do not teach or suggest a key in the form of an executable. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claim 11

Claim 11 recites a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising [emphasis added]:

- generating a new key with an incremented version number;
- sending the new key to a partner site for use in decoding tickets with the incremented version number;
- updating key and version information for a login server; and
- generating tickets decodable by the new key when an indication that a key having a previous version number has expired;
- wherein ***said keys comprise key data and executable code for decrypting tickets.***

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claim 12

Claim 12 recites a computer readable medium having instructions stored

thereon for causing a computer to perform a method of updating keys that decrypt login tickets that log a user into multiple sites, the method comprising [emphasis added]:

- generating a new key with an incremented version number;
- sending the new key to a partner site for use in decoding tickets with the incremented version number;
- updating key and version information for a login server; and
- generating tickets decodable by the new key when an indication that a key having a previous version number has expired;
- wherein ***said keys comprise key data and executable code for decrypting tickets***.

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claims 13 and 15

Claim 13 recites a method of updating a key used to decrypt tickets used to log into a site, the method comprising [emphasis added]:

- receiving an updated key with a new version number;
- setting a time for an old current key having an old version number to expire;
- making the updated key the current key;
- wherein ***at least one of said keys comprise executable code for making the updated key the current key.***

In making out the rejection of this claim, the Office states that the combination of Brown and Olkin does not teach "at least one of the keys comprise executable code for making the updated key the current key." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown-Olin with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claim 15 depends from claim 13 and is allowable as depending from an allowable base claim. This claim is also allowable for its own recited features which, in combination with those recited in claim 13, are neither disclosed nor suggested by the references as cited and applied by the Office.

Claim 16

Claim 16 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of updating a key used to

decrypt tickets used to log into a site, the method comprising [emphasis added]:

- receiving an updated key with a new version number;
- setting a time for an old current key having an old version number to expire;
- making the updated key the current key;
- wherein ***wherein at least one of said keys comprise executable code for making the updated key the current key.***

In making out the rejection of this claim, the Office states that the combination of Brown and Olkin does not teach "at least one of the keys comprise executable code for making the updated key the current key." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown-Olin with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claim 19-25

Claim 19 recites a method of managing keys used to decrypt tickets for logging onto a site, the method comprising:

- receiving a first key with a first version number;
- encrypting the first key using a hardware address;
- changing a current key variable to the first version number;

- receiving a new key with an incremented version number;
- encrypting the new key using a hardware address; and
- identifying the new key as the current key.

In making out the rejection of this claim, the Office restates its argument from the previous Office Action without responding to Applicant's response thereto. Applicant's previous response to the Office's argument is reproduced below for the Office's convenience:

> In making out the rejection of this claim, the Office argues that Brown discloses all of the features of the claim except for encrypting the first key and the new key using a hardware address. The Office then relies on Sherer for this feature, citing to column 7, lines 35-37, and argues that the combination of these references renders the subject matter of this claim obvious. Applicant respectfully disagrees and traverses the Office's rejection.
>
> In making out the rejection of this claim, the Office appears to argue, citing to the Specification on page 10, lines 2-4, that the recited feature "encrypting the new key using a hardware address" simply refers to storing the key using a piece of information that is specific to the physical machine, such as the MAC address of the first network card. Applicant respectfully disagrees and refers the Office to page 11, lines 22-23 which states: "[k]eydata contains the actual keys, encrypted in the HMAC of the machine."
>
> Sherer simply discloses that a so-called "star interconnection device stores, or otherwise has access to a certificate binding a MAC address on a port to a public key." This in no way discloses or suggests encrypting a new key using a hardware address.
>
> Accordingly, for at least this reason, the Office has failed to establish a *prima facie* case of obviousness and this claim is allowable.

Applicant is doing its best to further prosecution of this application but can do nothing but repeat its previous argument until the Office responds. Accordingly, Applicant respectfully requests the Office to either withdraw the rejection of this claim or to respond to Applicant's argument.

Claims 20-25 depend from claim 19 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 19, are neither disclosed nor suggested by the references as cited and applied by the Office. In addition, given the Office's failure to establish a *prima facie* case of obviousness with respect to claim 19, the further rejections of claims 20-22 over Olkin, of claim 23 over Olkin and Wasserman, and claim 25 over Audebert are not seen to add anything of significance.

Claim 26

Claim 26 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of managing keys used to decrypt tickets for logging onto a site, the method comprising [emphasis added]:

- receiving a first key with a first version number;
- ***encrypting the first key using a hardware address***;
- changing a current key variable to the first version number;
- receiving a new key with an incremented version number;
- ***encrypting the new key using a hardware address***; and
- identifying the new key as the current key.

In making out the rejection of this claim, the Office restates its argument from the previous Office Action without responding to Applicant's response thereto. Applicant's previous response to the Office's argument is reproduced below for the Office's convenience:

> In making out the rejection of this claim, the Office argues that Brown discloses all of the features of the claim except for encrypting the first key and the new key using a hardware address. The Office then relies on Sherer for

this feature and argues that the combination of these references renders the subject matter of this claim obvious. Applicant respectfully disagrees and traverses the Office's rejection.

As noted above, Sherer neither discloses nor suggests encrypting keys using a hardware address. Accordingly, for at least this reason, the Office has failed to establish a *prima facie* case of obviousness and this claim is allowable.

Applicant is doing its best to further prosecution of this application but can do nothing but repeat its previous argument until the Office responds. Accordingly, Applicant respectfully requests the Office to either withdraw the rejection of this claim or to respond to Applicant's argument.

Claims 27-33 and 35

Claim 27 recites a method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising [emphasis added]:

- generating a new key with a new version number to take the place of an old key with an old version number;
- storing the new key on a site to be logged into by a user;
- changing a current key indication to the new key;
- allowing current logged in users to continue using the old key; and
- redirecting new users to a login server to obtain a ticket consistent with the new key;
- ***wherein keys are generated in an executable form which includes key information as well as code for decrypting tickets using the key information.***

In making out the rejection of this claim, the Office argues that the combination of Brown, Audebert and Kandansky render the claimed subject matter obvious. However, ***nowhere*** in the rejection of this claim does the Office argue any of the cited references teaches ***keys are generated in an executable form***

which includes key information as well as code for decrypting tickets using the key information. Applicant respectfully submits that this omission is understandable, given the fact that none of the cited references even ***hint*** at ***keys generated in an executable form which includes key information as well as code for decrypting tickets using the key information***. Because the Office failed to argue that ***all*** of Applicant's claim features are met, and, because such claim features are not disclosed or suggested by the references, the Office has failed to make a *prima facie* case of obviousness.

Accordingly, for at least these reasons, this claim is allowable.

Claims 28-33 and 35 depend from claim 27 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 27, are neither disclosed nor suggested by the references as cited and applied by the Office. In addition, in view of the Office's failure to establish a *prima facie* case of obviousness with respect to claim 27, the rejections of claim 29 over the combination with Wasserman, and of claim 32 over Olkin and Biran is not seen to add anything of significance.

Claim 36

Claim 36 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of updating keys used to decrypt tickets used to log into multiple sites on a network, the method comprising [emphasis added]:

- generating a new key with a new version number to take the place of an old key with an old version number;

- storing the new key on a site to be logged into by a user;
- changing a current key indication to the new key;
- allowing current logged in users to continue using the old key; and
- redirecting new users to a login server to obtain a ticket consistent with the new key,
- ***wherein the keys comprise key data and executable code for decrypting tickets.***

In making out the rejection of this claim, the Office argues that the combination of Brown, Audebert and Kandansky render the claimed subject matter obvious. However, ***nowhere*** in the rejection of this claim does the Office argue any of the cited references teaches that ***keys comprise key data and executable code for decrypting tickets***. Applicant respectfully submits that this omission is understandable, given the fact that none of the cited references even ***hint*** at ***keys comprising key data and executable code for decrypting tickets.*** Because the Office failed to argue that ***all*** of Applicant's claim features are met, and, because such claim features are not disclosed or suggested by the references, the Office has failed to make a *prima facie* case of obviousness.

Accordingly, for at least these reasons, this claim is allowable.

Claims 37-40

Claim 37 recites a method of logging on to multiple sites, the method comprising [emphasis added]:

- sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;
- receiving an indication that the first key has expired;
- obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and

- sending the second login ticket to the site to log into the site;
- wherein ***the keys comprise key data and executable code for decrypting tickets.***

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claims 38-40 depend from claim 37 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 37, are neither disclosed nor suggested by the references as cited and applied by the Office.

Claim 41

Claim 41 recites a computer readable medium having instructions stored thereon for causing a computer to perform a method of logging on to multiple sites, the method comprising [emphasis added]:

- sending a first login ticket to a desired site, wherein the login ticket is encrypted to be decoded by a first key having a first version number;

- receiving an indication that the first key has expired;
- obtaining a second login ticket from an authentication server, wherein the second login ticket is encrypted consistently with a new key having a second version number; and
- sending the second login ticket to the site to log into the site;
- wherein ***the keys comprise key data and executable code for decrypting tickets.***

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Claim 42

Claim 42 recites an encrypted ticket for use in logging on to a website, the ticket comprising [emphasis added]:

- an unencrypted version number corresponding to a key version number stored on the website; and
- an encrypted string identifying the website and information, which when decrypted using the key having the same version number authenticates the user for logging the user into the website;
- wherein ***the key comprises executable code for decrypting tickets.***

In making out the rejection of this claim, the Office states that Brown does not teach that "the key comprises key data and executable code for decrypting tickets." Applicant agrees. The Office then argues that Moreau teaches "the use of a key in the form of an executable." The Office further argues that it would have been obvious to "modify the teaching of Brown with the teachings of Moreau to include a key in the form of an executable with the motivation to improve the security of the system."

As noted above, the combination of these references does not teach or suggest all of the claim features. Accordingly, the Office has failed to establish a *prima facie* case of obviousness and, for at least this reason, this claim is allowable.

Conclusion

Applicant respectfully submits that all of the claims are in condition for allowance. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 1/25/2005 By: Reg. No. 38605 for Rob Cottle

Rob R. Cottle
Reg. No. 52,772
(509) 324-9256